PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-063076
(43)Date of publication of application : 28.02.2002

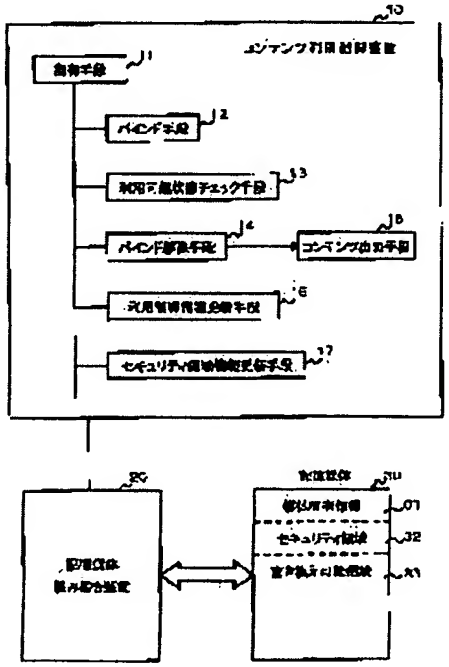
(51)Int.Cl. G06F 12/14
G11B 20/10
H04N 5/91
H04N 5/93
H04N 7/167

(21)Application number : 2000-249304
(22)Date of filing : 21.08.2000

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : IORI SACHIKO
MIYAKE NOBUHISA
NAKAZATO KANA
FUJII HARUHIKO

(54) CONTENT USE CONTROL METHOD, CONTENT USE CONTROLLER, STORAGE MEDIUM FOR CONTENT USE CONTROL PROGRAM, AND STORAGE MEDIUM FOR CONTENT

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent replay attack by a method, where contents stored in a storage medium are backed up; when the number of their uses is limited and a means is provided for making the backup contents unusable, even if they are returned to the original storage medium, after the contents have been used.
SOLUTION: The usable state of the contents reserved in the storage medium 30 are bound, by using information in a security area 32 provided in the storage medium 30. Each time the contents in the storage medium 30 are reproduced, the information in the security area 32 is rewritten to re-bind the usable state of the contents. Only when the information in the security area 32 has the value held when the bind is made, is the bound information enabled. If the information in the security area 32 is different from the value held when the bind is made, the bound information is disabled.



LEGAL STATUS

[Date of request for examination] 21.08.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－63076
(P2002－63076A)
(43)公開日　平成14年２月28日(2002.2.28)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０１７
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｃ０５３
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ	５Ｃ０６４
5/93		5/93	Ｚ	５Ｄ０４４
7/167		7/167	Ｚ	

審査請求　有　請求項の数６　ＯＬ　（全 11 頁）

(21)出願番号　特願2000－249304(P2000－249304)

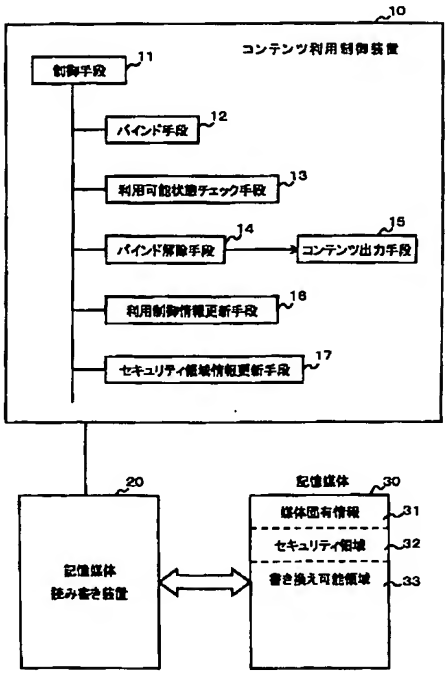
(22)出願日　平成12年８月21日(2000.8.21)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　庵　祥子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　三宅　延久
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100087848
弁理士　小笠原　吉義　（外２名）

最終頁に続く

(54)【発明の名称】　コンテンツ利用制御方法，コンテンツ利用制御装置，コンテンツ利用制御プログラム記憶媒体およびコンテンツ記憶媒体

(57)【要約】
【課題】　記憶媒体に格納されているコンテンツの利用回数が制限されている場合に，バックアップをとり，コンテンツを利用した後にそのバックアップコンテンツを元の記憶媒体に戻しても利用不可能とする手段を設け，リプレイアタックを防止する。
【解決手段】　記憶媒体30に保存されているコンテンツの利用可能状態を記憶媒体30に設けたセキュリティ領域32の情報を用いてバインドし，記憶媒体30上のコンテンツを再生するたびにセキュリティ領域32の情報を書き換えてコンテンツの利用可能状態をバインドし直す。セキュリティ領域32の情報がバインド時の値を持つ場合にのみバインドされた情報を有効とし，セキュリティ領域32の情報がバインド時の値と異なっていれば，バインドされた情報を無効とする。



【特許請求の範囲】

【請求項１】　記憶媒体に格納されたコンテンツの利用回数を，そのコンテンツに付随する利用制御情報によって制御する方法において，前記記憶媒体に可逆的な更新ができないセキュリティ領域を設け，前記記憶媒体中のコンテンツ，利用制御情報またはその他のコンテンツの利用に必要な情報を，前記セキュリティ領域の情報にバインドさせることにより，前記セキュリティ領域の情報がバインド時の値を持つ場合にのみバインドされた情報が有効となるようにし，前記記憶媒体中のコンテンツの利用要求に対して，その利用制御情報における残り利用回数を読み出して利用可能状態であることを確認し，前記記憶媒体中のセキュリティ領域の情報を利用して前記バインドを解くことにより前記コンテンツを利用に供し，前記利用制御情報における残り利用回数を更新し，前記セキュリティ領域の情報を前の値と異なる値に変更し，前記記憶媒体中のコンテンツ，利用制御情報またはその他のコンテンツの利用に必要な情報を，前記セキュリティ領域の情報で再バインドすることを特徴とするコンテンツ利用制御方法。

【請求項２】　前記記憶媒体は，それぞれの記憶媒体に固有の媒体固有情報を持ち，前記記憶媒体に格納されたコンテンツは変形または暗号化されており，前記媒体固有情報を用いて復元可能になっていることを特徴とする請求項１記載のコンテンツ利用制御方法。

【請求項３】　各記憶媒体に固有の媒体固有情報の記憶部と，媒体固有情報を用いて変形された変形コンテンツおよびそのコンテンツの利用可能状態を示す管理テーブルとが格納された書き換え可能領域と，コンテンツの利用状況に応じて特定の値を保持するセキュリティ領域とを有する記憶媒体から，コンテンツに関する情報を読み出して，利用回数制限付きのコンテンツの利用を制御する方法であって，前記記憶媒体中の管理テーブルを前記セキュリティ領域の情報にバインドさせることにより，前記セキュリティ領域の情報がバインド時の値を持つ場合にのみ管理テーブル中の情報が有効となるようにし，コンテンツの利用要求に対して前記セキュリティ領域の情報を読み出し，利用要求があったコンテンツの利用状態が利用可能状態であることを前記セキュリティ領域の情報と前記管理テーブルにより確認し，前記記憶媒体の媒体固有情報を読み出し，前記記憶媒体の媒体固有情報と変形コンテンツを利用することにより復元したコンテンツを出力し，前記管理テーブルおける出力したコンテンツの残り利用回数を更新し，前記セキュリティ領域の情報を変化させ，前記管理テーブルを前記セキュリティ領域の情報を利用して再バインドすることを特徴とするコンテンツ利用制御方法。

【請求項４】　記憶媒体に格納されたコンテンツの利用回数を，そのコンテンツに付随する利用制御情報によって制御する装置において，前記記憶媒体中のコンテンツ，利用制御情報またはその他のコンテンツの利用に必要な情報を，前記記憶媒体中に設けられた可逆的な更新ができないセキュリティ領域の情報にバインドさせることにより，前記セキュリティ領域の情報がバインド時の値を持つ場合にのみバインドされた情報が有効となるようにするバインド手段と，前記記憶媒体中のコンテンツの利用要求に対して，その利用制御情報における残り利用回数を読み出して利用可能状態であることを確認する利用可能状態チェック手段と，前記記憶媒体中のセキュリティ領域の情報を利用して前記バインドを解くことにより前記コンテンツを利用可能とするバインド解除手段と，前記コンテンツの利用ごとに前記利用制御情報における残り利用回数を更新する利用制御情報更新手段と，前記コンテンツの利用ごとに前記セキュリティ領域の情報を前の値と異なる値に変更するセキュリティ領域情報変更手段とを備え，前記バインド手段は，前記コンテンツの利用によりセキュリティ領域の情報が変更されるごとに，前記記憶媒体中のコンテンツ，利用制御情報またはその他のコンテンツの利用に必要な情報を，前記セキュリティ領域の情報で再バインドすることを特徴とするコンテンツ利用制御装置。

【請求項５】　記憶媒体に格納されたコンテンツの利用回数を，そのコンテンツに付随する利用制御情報によって制御するためのプログラムを格納した記憶媒体であって，前記記憶媒体中のコンテンツ，利用制御情報またはその他のコンテンツの利用に必要な情報を，前記記憶媒体中に設けられた可逆的な更新ができないセキュリティ領域の情報にバインドさせることにより，前記セキュリティ領域の情報がバインド時の値を持つ場合にのみバインドされた情報が有効となるようにする処理と，前記記憶媒体中のコンテンツの利用要求に対して，その利用制御情報における残り利用回数を読み出して利用可能状態であることを確認する処理と，前記記憶媒体中のセキュリティ領域の情報を利用して前記バインドを解くことにより前記コンテンツを利用に供する処理と，前記利用制御情報における残り利用回数を更新する処理と，前記セキュリティ領域の情報を前の値と異なる値に変更する処理と，前記記憶媒体中のコンテンツ，利用制御情報またはその他のコンテンツの利用に必要な情報を，前記セキュリティ領域の情報で再バインドする処理とを，コンピュータに実行させるためのプログラムを格納したことを特徴とするコンテンツ利用制御プログラム記憶媒体。

【請求項６】　利用制御情報によって利用回数が制限されたデジタルコンテンツが格納された記憶媒体であって，各記憶媒体に固有の媒体固有情報の記憶部と，前記媒体固有情報を用いて変形された変形コンテンツおよびそのコンテンツの利用制御情報とが格納された書き換え可能領域と，コンテンツの利用状況に応じて特定の値を保持する領域であって，少なくとも前記コンテンツの利用によって前記書き換え可能領域が更新されるごとに領

域中の前記特定の値が非可逆的に変更され，前記書き換え可能領域中の情報を前記変更された値にバインドさせることにより，バインドされた前記書き換え可能領域中の情報を，前記特定の値がバインド時の値である場合にのみ有効とするための情報を保持するセキュリティ領域とを有することを特徴とするコンテンツ記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，記憶媒体の固有情報を用いて変形されたデジタルコンテンツを利用する端末において，リプレイアタックを防止して利用回数を制御した再生を可能とするコンテンツ利用制御方法に関するものである。

【０００２】

【従来の技術】画像情報，音楽情報，テキスト情報，ソフトウェアプログラムなどの各種のデジタルコンテンツが，携行可能な記憶媒体に格納されて利用されることが多くなってきており，その記憶媒体の商品化も進んでいる。例えば，“SolidAudio”（登録商標）と呼ばれる商品は，音楽データを格納し，プレーヤによって再生を可能にした記憶媒体である。

【０００３】このような記憶媒体上のコンテンツの利用制御方法として，特に著作権の保護のため，記憶媒体の固有情報をもとにコンテンツを変形させて利用制御する方法が用いられている。しかしながらこの方法では，特定の記憶媒体に保存してしまったコンテンツは何度でも利用することが可能であり，利用回数を制御することができないという問題があった。

【０００４】これに対し，コンテンツに利用制御情報を付加し，利用回数を制御するという方法があるが，この場合，記憶媒体の固有情報で変形されたコンテンツのバックアップを，他の記憶媒体にとり，記憶媒体上のコンテンツを利用制御情報によって制御されている利用回数分再生し終わったあと，再びバックアップを保存しておいた他の記憶媒体から元の記憶媒体にバックアップを戻した場合，元の記憶媒体で再びコンテンツが利用可能になってしまう，すなわちリプレイアタックができてしまうという問題があった。

【０００５】

【発明が解決しようとする課題】本発明の目的は，記憶媒体に保存されているコンテンツの利用可能状態を記憶媒体に設けたセキュリティ領域の情報を用いてバインドし，記憶媒体上のコンテンツを再生するたびにセキュリティ領域の情報を書き換えてコンテンツの利用可能状態をバインドし直すことにより，たとえ記憶媒体上でコンテンツを再生する前にそのコンテンツのバックアップが他の記憶媒体に取られていたとしても，セキュリティ領域の情報が変化され利用可能状態がその情報に基づいてバインドし直されているため，そのバックアップコンテンツを記憶媒体に戻しても利用不可能になっていることにより，リプレイアタックを防いだ利用回数制御付きコンテンツ再生を可能とすることにある。

【０００６】

【課題を解決するための手段】本発明は，記憶媒体の媒体固有情報を利用して変形されているコンテンツの利用回数制御付き再生において，コンテンツの利用可能状態を，記憶媒体上にセキュリティ領域を設けて，その領域の情報を利用して管理することにより，記憶媒体の媒体固有情報を利用して変形されているコンテンツをリプレイアタックを防止しつつ利用回数制御付き再生可能とすることを主な特徴とする。

【０００７】上記の目的を達成するための方法として，コンテンツ記憶媒体は，少なくとも書き換え可能領域と，可逆的な更新ができないセキュリティ領域とを持つものとし，またコンテンツを変形（暗号化を含む）して格納する場合には，コンテンツの変形に用いるための各記憶媒体に固有の媒体固有情報を持つものとする。

【０００８】書き換え可能領域には，記憶媒体の媒体固有情報を利用して変形された変形コンテンツと利用制御情報，あるいは暗号化コンテンツと記憶媒体の媒体固有情報を利用して変形された変形復号鍵と利用制御情報とが保存されるものとする。これらの情報は１つにまとめられていても別々に保存されていても構わない。別々に保存されている場合には変形コンテンツから利用制御情報へ，あるいは暗号化コンテンツから変形復号鍵と利用制御情報へのリンク情報と認証情報を持つものとする。

【０００９】コンテンツの利用可能状態の管理にコンテンツ利用可能状態管理テーブルを利用する場合には，この管理テーブルにコンテンツへのリンク情報と利用可能状態を示す情報が管理されているものとする。また，変形コンテンツあるいは暗号化コンテンツは，管理テーブルへのリンク情報を持つものとする。

【００１０】以下，記憶媒体上のコンテンツを再生する場合を例にとって説明する。記憶媒体には，記憶媒体の媒体固有情報を利用して変形された変形コンテンツ，または暗号化コンテンツと記憶媒体の媒体固有情報を利用して変形された変形復号鍵，さらに利用制御情報が保存されているものとする。また，変形コンテンツあるいは変形復号鍵は，それぞれが保存されている記憶媒体のセキュリティ領域の情報によって利用可能状態がバインドされているものとする。

【００１１】まず，記憶媒体のセキュリティ領域の情報を読み出し，この情報と改ざん検出機能付き利用制御情報を用いて記憶媒体に保存されているコンテンツが利用可能状態であることを確認する。利用可能であった場合，セキュリティ領域の情報を用いてコンテンツのバインドを解き，記憶媒体の媒体固有情報を読み出し，この媒体固有情報と変形コンテンツを利用してコンテンツの再生を行う。また利用制御情報の残り利用回数を変更する。さらにセキュリティ領域の情報を書き換え，新しい

セキュリティ領域の情報で記憶媒体上の全てのコンテンツをバインドし直す。

【００１２】コンテンツの再生とセキュリティ領域の書き換え等については，リプレイアタックを防止した利用回数制限付き再生が実現可能な場合に限り，順番が前後しても構わない。

【００１３】記憶媒体上にコンテンツ利用可能状態管理テーブルが存在する場合には，まず記憶媒体のセキュリティ領域の情報を読み出し，この情報とコンテンツ利用可能状態管理テーブルを用いて記憶媒体上に保存されている再生しようとしているコンテンツが利用可能状態であることを確認する。利用可能であった場合，セキュリティ領域の情報を用いてコンテンツ利用可能状態管理テーブルのバインドを解く。また記憶媒体の媒体固有情報を読み出し，この媒体固有情報と変形コンテンツを利用してコンテンツの再生を行う。さらに利用制御情報の残り利用回数を変更する。そしてセキュリティ領域の情報を書き換え，新しいセキュリティ領域の情報でコンテンツ利用可能状態管理テーブルをバインドし直す。

【００１４】コンテンツの再生とセキュリティ領域の情報の書き換え等については，リプレイアタックを防止した利用回数制限付き再生方法が実現可能な場合に限り，順番が前後しても構わない。

【００１５】もし他の記憶媒体に，記憶媒体上にある変形コンテンツやコンテンツ利用可能状態管理テーブル等のバックアップを取って置いたとしても，少なくともどれか１つのコンテンツを再生することによってセキュリティ領域の情報が変更され，それに伴いコンテンツあるいはコンテンツ利用可能状態管理テーブルが再バインドされてしまうため，バックアップされていた変形コンテンツやコンテンツ利用可能状態管理テーブルは利用不可能となる。これにより，リプレイアタックを防止したコンテンツの利用回数制限付き再生を可能にする。

【００１６】コンテンツは，静止画像，動画像，音楽，テキストなどのデータや，ソフトウェアプログラムであり，あらかじめ暗号化された暗号化コンテンツとその復号鍵でも構わない。この場合，復号鍵を記憶媒体の媒体固有情報を用いて変形し変形復号鍵にするものとする。暗号化コンテンツが記憶媒体の媒体固有情報を用いて変形されていてもよい。

【００１７】コンテンツ，暗号化コンテンツ，復号鍵の変形では，暗号化処理，スクランブル処理またはハッシュ処理を少なくとも１回以上行うものとし，記憶媒体内の情報をセキュリティ領域の情報とともに変形に用いても構わない。

【００１８】コンテンツ利用可能状態管理テーブルを利用する場合，変形コンテンツあるいは暗号化コンテンツは，コンテンツ利用可能状態管理テーブルに対するリンク情報を持つものとする。

【００１９】改ざん検出機能付き利用制御情報とは，利用制御情報のデジタル署名またはチェックサムを利用制御情報に付加したもの，あるいは個別に保存したものである。また，改ざん検出機能付き利用制御情報は，変形コンテンツや変形復号鍵に内包されていても構わない。また，変形されていても構わないものとする。

【００２０】記憶媒体は媒体固有情報を有し，少なくとも書き換え可能領域とセキュリティ領域を持つ。また，記憶媒体の媒体固有情報は，利用者が書き換え不可能あるいは書き換え困難な領域に保存されているものとする。

【００２１】セキュリティ領域は，１度しか書きこめない領域，あるいは複数回の書き込みが困難な領域であり，この領域に書き込むアドレスの順序に決まりがあるようなものでもよい。あるいはカウントアップのみを許可した領域であっても構わない。

【００２２】コンテンツ利用可能状態管理テーブルは，記憶媒体上の書き換え可能領域でコンテンツの利用可能状態を管理し，コンテンツ利用可能状態管理テーブルに記載する情報は少なくともコンテンツと対応の取れる情報と利用可能回数あるいは利用済回数を含むものとする。また，コンテンツの利用可能状態が変化した場合には，利用可能回数あるいは利用済回数をそのたびに書き換えることが可能なものとする。また，変形コンテンツ，暗号化コンテンツあるいは変形復号鍵からコンテンツ利用可能状態管理テーブルを参照するためのリンク情報と認証情報を持つものとする。

【００２３】変形コンテンツとコンテンツ利用可能状態管理テーブルの少なくとも一方は，セキュリティ領域の情報を利用してバインドして保存するものとする。例えば，ある情報Ａを情報Ｂにバインドするとは，情報Ｂがバインド時の値を持つ場合にのみ情報Ａが有効になるように制約を加えることである。バインドを解く（またはバインドを復元する）とは，制約を解除して情報Ａを利用可能にすることである。バインドでは，暗号化処理，スクランブル処理，電子署名処理，ハッシュ処理またはチェックサム処理を少なくとも１回以上行うものとする。さらに記憶媒体内の情報をセキュリティ領域の情報とともに変形に利用しても構わないものとする。また，セキュリティ領域の情報が変化するたびに，バインド対象の情報をバインドし直すものとする。

【００２４】変形コンテンツ（または暗号化コンテンツと変形復号鍵），改ざん検出機能付き利用制御情報は，１つにまとめられていても，別々に保存されていてもよい。別々に保存されている場合には，変形コンテンツが利用制御情報に対するリンク情報を持つ，あるいは暗号化コンテンツが変形復号鍵と利用制御情報のそれぞれに対するリンク情報を持つものとする。

【００２５】コンテンツ再生残り利用回数がゼロになった場合には，記憶媒体からコンテンツに関する情報を消去してもよく，またはそのまま残しておいてもよい。

【００２６】コンテンツの残り利用回数の変更は，コンテンツ再生の始め，終わり，あるいは指定された割合を再生したときであっても構わないものとする。ここで，残り利用回数の変更では，今まで何回再生したかをカウントアップする方法を用いてもよい。

【００２７】本発明の作用は，以下のとおりである。コンテンツの利用可能状態をセキュリティ領域の情報にバインドし，記憶媒体上にあるコンテンツを利用回数制御付きの再生を行う場合に，セキュリティ領域の情報を変化させて他の変形コンテンツあるいはコンテンツ利用可能状態管理テーブルの再バインドを行うことにより，他の記憶媒体上に記憶媒体の変形コンテンツやコンテンツ利用可能状態管理テーブルのバックアップを取っておき，それを記憶媒体に戻してもコンテンツを利用することを不可能にしている。これによりリプレイアタックを防止した利用回数制限付き再生を実現することが可能となり，本発明の目的であるコンテンツの利用制御を行うことができるようになる。

【００２８】図１は，本発明の構成例を示す図である。コンテンツ利用制御装置１０は，制御手段１１，バインド手段１２，利用可能状態チェック手段１３，バインド解除手段１４，コンテンツ出力手段１５，利用制御情報更新手段１６，セキュリティ領域情報更新手段１７を持つ。これらの各手段は，コンピュータとソフトウェアプログラム等によって構成される。このソフトウェアプログラムは，コンピュータが読み取り可能な可搬媒体メモリ，半導体メモリ，ハードディスクなどの適当な記憶媒体に格納することができる。

【００２９】記憶媒体３０は，静止画像，動画像，音楽，テキストなどのデータや，ソフトウェアプログラム等のデジタルコンテンツが格納される媒体であり，記憶媒体読み書き装置２０は，記憶媒体３０のデータを読み出したり書き込んだりする装置である。記憶媒体３０は，各記憶媒体に固有に割り当てられた媒体固有情報３１と，可逆的な更新ができないセキュリティ領域３２と，コンテンツやその利用制御情報，さらに場合によっては，コンテンツ利用可能状態管理テーブル，復号鍵などの情報が格納される書き換え可能領域３３を持つ。

【００３０】制御手段１１は，コンテンツ利用制御装置１０の全体を制御する手段である。バインド手段１２は，記憶媒体３０中のコンテンツ，利用制御情報またはその他のコンテンツの利用に必要な情報を，セキュリティ領域３２の情報にバインドさせることにより，セキュリティ領域３２の情報がバインド時の値を持つ場合にのみバインドされた情報が有効となるようにする手段である。

【００３１】利用可能状態チェック手段１３は，記憶媒体３０中のコンテンツの利用要求に対して，その利用制御情報における残り利用回数を読み出して利用可能状態であることを確認する手段である。残り利用回数が０である場合には，利用要求を拒否する。バインド解除手段１４は，記憶媒体３０中のセキュリティ領域３２の情報を利用してバインドを解くことにより，要求されたコンテンツをコンテンツ出力手段１５を介して出力する。

【００３２】利用制御情報更新手段１６は，記憶媒体３０中のコンテンツが利用された場合に，書き換え可能領域３３に保持されている利用制御情報における残り利用回数を更新する。セキュリティ領域情報更新手段１７は，利用制御情報が更新されると，セキュリティ領域３２の情報を前の値と異なる値に変更する。その後，バインド手段１２は，記憶媒体３０中のコンテンツ，利用制御情報またはその他のコンテンツの利用に必要な情報を，セキュリティ領域３２の情報で再バインドする。

【００３３】

【発明の実施の形態】〔第１の実施の形態〕図２に，第１および第２の実施の形態に係るコンテンツ再生装置の構成例を示す。第１の実施の形態は，記憶媒体３０の書き換え可能領域３３中にコンテンツ利用可能状態管理テーブルを持たない場合の例である。

【００３４】コンテンツ再生装置１００は，記憶媒体３０に格納されたコンテンツを再生する装置である。記憶媒体３０は，コンテンツ再生装置１００に固定されているものでも，取り外し可能なものであっても構わないものとする。コンテンツ再生装置１００は，制御部１０１，セキュリティ領域情報読み出し・書き込み部１０２，コンテンツ利用可能状態確認部１０３，媒体固有情報読み出し部１０４，コンテンツバインド・復元部１０５，コンテンツ再生部１０６，利用制御情報書き換え部１０７を備える。

【００３５】記憶媒体３０の書き換え可能領域３３には，記憶媒体３０の媒体固有情報で暗号化された変形コンテンツと，この変形コンテンツの利用制御情報（残り利用回数＝３）が保存されているものとする。また，記憶媒体３０のセキュリティ領域３２の情報は０であるものとする。このコンテンツを再生する場合，制御部１０１の制御のもとに次のようにコンテンツを再生する。図３は，コンテンツ再生装置１００の処理フローチャートである。

【００３６】まず，セキュリティ領域情報読み出し・書き込み部１０２を利用して，記憶媒体３０のセキュリティ領域３２の情報を読み出す（図３のステップＳ１）。この時点のセキュリティ領域３２の情報は０である。そして，読み出した情報と変形コンテンツ，利用制御情報を利用してコンテンツ利用可能状態確認部１０３において，再生するコンテンツが利用可能状態にあるかどうかを確認する（ステップＳ２）。

【００３７】コンテンツが利用可能状態であった場合，コンテンツバインド・復元部１０５で記憶媒体３０のセキュリティ領域３２の情報を利用して，再生する変形コンテンツのバインドを解く（ステップＳ３）。さらに媒

体固有情報読み出し部１０４で記憶媒体３０の媒体固有情報３１を読み出し（ステップＳ４），この媒体固有情報３１と変形コンテンツを利用しコンテンツ再生部１０６でコンテンツを再生する（ステップＳ５）。そして，利用制御情報書き換え部１０７を利用して，再生したコンテンツの利用制御情報の残り利用回数を書き換える（ステップＳ６）。残り利用回数は３から２に更新される。書き換えのタイミングは，再生を始めたとき，あるいは再生が最後まで終わったとき，あるいは情報提供者の指定したタイミングであるものとする。

【００３８】その後，セキュリティ領域情報読み出し・書き込み部１０２で，記憶媒体３０のセキュリティ領域３２の情報を０から１に書き換え（ステップＳ７），コンテンツバインド・復元部１０５でこの書き換え後の情報を利用して記憶媒体３０上にある全ての変形コンテンツを再バインドする（ステップＳ８）。

【００３９】図４に，バインドの例を示す。バインド方法として，暗号化処理，スクランブル処理，電子署名処理，ハッシュ処理またはチェックサム処理など，各種の方法を用いることができるが，ここではハッシュ処理を用いた例を説明する。

【００４０】図４（Ａ）に示すように，セキュリティ領域３２には情報ａが格納され，書き換え可能領域３３中の被バインド情報にはＡが格納されていたとする。被バインド情報は，コンテンツ，利用制御情報または後述する例ではコンテンツ利用可能状態管理テーブルである。まず，ａとＡとを接続し，接続された情報全体に対して，所定のハッシュ関数を用いてハッシュ処理を施す。このハッシュ結果Ｘａを，書き換え可能領域３３中に保存しておく。

【００４１】このバインドを解除する場合，図４（Ｂ）に示すように，セキュリティ領域３２の情報ａと，書き換え可能領域３３における被バインド情報Ａとを接続し，バインド時と同じハッシュ関数を用いてハッシュ処理を行い，そのハッシュ結果Ｘａと書き換え可能領域３３に記憶しておいたバインド時のハッシュ結果Ｘａとを比較する。一致した場合には，被バインド情報Ａを有効なものとして扱う。

【００４２】例えば図４（Ｃ）に示すように，セキュリティ領域３２の情報がｂに変わっていたとすると，ハッシュ結果Ｘｂとバインド時のハッシュ結果Ｘａとは不一致となるため，被バインド情報Ａは無効データとして扱われる。

【００４３】例えば，セキュリティ領域３２の情報ａと被バインド情報Ａのそれぞれに対してハッシュ処理を行い，それらの出力結果を接続して，さらにそれに対してハッシュ処理を行うというようなハッシュ方法を用いてもよい。

【００４４】バインドの方法はこれに限らず，例えば暗号化処理を用いてバインドする場合には，セキュリティ領域の情報ａを鍵として，被バインド情報Ａを暗号化するというような方法を用いることができる。

【００４５】〔第２の実施の形態〕第２の実施の形態は，記憶媒体３０の書き換え可能領域３３中にコンテンツ利用可能状態管理テーブルを持たない場合で，書き換え可能領域３３中のコンテンツを暗号鍵で暗号化している場合の例である。

【００４６】記憶媒体３０の書き換え可能領域３３には，あらかじめ暗号化された暗号化コンテンツと，その復号鍵を記憶媒体３０の媒体固有情報で暗号化した変形復号鍵とが格納されている。また，この暗号化コンテンツの利用制御情報として，残り利用回数＝３の情報が保存されているとする。セキュリティ領域３２の情報は０であるとする。

【００４７】このコンテンツを再生するときの例について説明する。コンテンツ再生装置の構成は，図２と同様である。まず，セキュリティ領域情報読み出し・書き込み部１０２を利用して，記憶媒体３０のセキュリティ領域３２の情報を読み出す（この時点の情報は０）。そして，読み出した情報と変形復号鍵，利用制御情報を利用してコンテンツ利用可能状態確認部１０３において，再生するコンテンツが利用可能状態にあるかどうかを確認する。コンテンツが利用可能状態であった場合，コンテンツバインド・復元部１０５で記憶媒体３０のセキュリティ領域３２の情報を利用して変形復号鍵のバインドを復元する。さらに媒体固有情報読み出し部１０４で記憶媒体３０の媒体固有情報３１を読み出し，この媒体固有情報３１と変形復号鍵と暗号化コンテンツを利用し，コンテンツ再生部１０６でコンテンツを再生する。

【００４８】利用制御情報書き換え部１０７を利用して，再生したコンテンツの利用制御情報の残り利用回数を書き換える。残り利用回数は，３から２に更新される。書き換えのタイミングは，再生を始めたとき，あるいは再生が最後まで終わったとき，あるいは情報提供者の指定したタイミングであるものとする。また，記憶媒体３０のセキュリティ領域３２の情報を書き換え（この時点の情報は１），コンテンツバインド・復元部１０５でこの書き換え後の情報を利用して，記憶媒体３０上にある全ての変形復号鍵を再バインドする。

【００４９】〔第３の実施の形態〕図５に，第３および第４の実施の形態に係るコンテンツ再生装置の構成例を示す。第３の実施の形態は，記憶媒体３０の書き換え可能領域３３中にコンテンツ利用可能状態管理テーブルを持つ場合の例である。

【００５０】コンテンツ再生装置１１０は，記憶媒体３０に格納されたコンテンツを再生する装置である。記憶媒体３０は，コンテンツ再生装置１１０に固定されているものでも，取り外し可能なものであっても構わない。コンテンツ再生装置１１０は，制御部１１１，セキュリティ領域情報読み出し・書き込み部１１２，コンテンツ

利用可能状態確認部１１３，媒体固有情報読み出し部１１４，管理テーブルバインド・復元部１１５，コンテンツ再生部１１６，管理テーブル読み出し・書き込み部１１７を備える。

【００５１】記憶媒体３０の書き換え可能領域３３には，記憶媒体３０の媒体固有情報３１で暗号化された変形コンテンツと，この変形コンテンツの利用可能状態を管理するコンテンツ利用可能状態管理テーブルが保存されている。なお，コンテンツ利用可能状態管理テーブル以外にも，使用期限その他の利用制御情報を持つこともできる。

【００５２】図６に，コンテンツ利用可能状態管理テーブルの構成例を示す。図６（Ａ）は，コンテンツ利用回数ごとに情報を持つ場合の例を示している。この例では，コンテンツ１とコンテンツ２は，２回利用可能であり，コンテンツ３は１回利用可能なコンテンツであったことを表している。このうち，コンテンツ１－１の利用可能フラグは０になっており，コンテンツ１は既に１回利用されていることが記されている。使用済みフラグは，テーブルのそのエリアが既に使用されているのかそれともまだ使用されていないのかを表すフラグである。このフラグが１の場合，テーブルの情報は有効であり，０の場合，未使用であるため情報は無効である。

【００５３】図６（Ｂ）は，コンテンツごとに利用回数の情報を持つ場合で，この例では，コンテンツ１とコンテンツ３の残り利用回数が１回，コンテンツ２の残り利用回数が１回となっている。この方式では，残り利用回数はわかるが，最初の利用可能回数はわからないようになっている。

【００５４】図５のコンテンツ再生装置１１０において，今回再生対象とするコンテンツの残り利用回数は３であるものとする。また，記憶媒体３０のセキュリティ領域３２の情報は０であるものとする。

【００５５】このコンテンツを再生するときの例について説明する。まず，セキュリティ領域情報読み出し・書き込み部１１２を利用して記憶媒体３０のセキュリティ領域３２の情報を読み出す（この時点の情報は０）。また，管理テーブル読み出し・書き込み部１１７を利用してコンテンツ利用可能状態管理テーブルを読み出す（この時点で再生対象コンテンツの残り利用回数は３）。そして，読み出したセキュリティ領域３２の情報とコンテンツ利用可能状態管理テーブルと変形コンテンツとを利用して，コンテンツ利用可能状態確認部１１３において，再生するコンテンツが利用可能状態にあるかどうかを確認する。コンテンツが利用可能状態であった場合，媒体固有情報読み出し部１１４で記憶媒体３０の媒体固有情報３１を読み出し，この媒体固有情報３１と変形コンテンツを利用し，コンテンツ再生部１１６でコンテンツを再生する。

【００５６】また，管理テーブルバインド・復元部１１５でセキュリティ領域３２の情報を利用して，コンテンツ利用可能状態管理テーブルのバインドを復元する。そして管理テーブル読み出し・書き込み部１１７を利用して，コンテンツ利用可能状態管理テーブル内の再生したコンテンツの残り利用回数を書き換える。残り利用回数は３から２となる。書き換えのタイミングは，再生を始めたとき，あるいは再生が最後まで終わったとき，あるいは情報提供者の指定したタイミングであるものとする。

【００５７】さらに，記憶媒体３０のセキュリティ領域３２の情報を書き換え（この時点の情報は１），管理テーブルバインド・復元部１１５でこの書き換え後の情報を利用して，記憶媒体３０上のコンテンツ利用可能状態管理テーブルを再バインドする。

【００５８】コンテンツ利用可能状態管理テーブルがセキュリティ領域３２の情報でバインドされるので，コンテンツ利用可能状態管理テーブルはバインド時のセキュリティ領域３２の情報のときにのみ有効である。図４で説明したように，コンテンツ利用可能状態管理テーブルに，コンテンツ利用可能状態管理テーブルとセキュリティ領域情報を連結した情報のハッシュ処理結果，デジタル署名またはチェックサムを付加し，ハッシュ処理結果，デジタル署名またはチェックサムが正しいときだけ，コンテンツ利用可能状態管理テーブルを利用するようにすることによりバインドを実現することができる。

【００５９】セキュリティ領域３２として，書き込みが一度だけ可能であって，書き込みアドレスの順序が低いアドレスから高いアドレスに書き込める制約があり，その領域の初期値として，全てのアドレスの内容が０である場合には，次のように実現する。セキュリティ領域３２の情報としては，セキュリティ領域３２の各アドレスで非０の数を考える。領域の初期値として，全てのアドレスの内容が０であるので，初期値は０となる。続いて，セキュリティ領域３２を変化させる場合には，低いアドレス（例えば０番地）の値を，０から１に変更する。そうすると，非０の数は１となるので，セキュリティ領域情報は，１となる。さらに変化させる場合には，１番地の内容を，１に，２番地の内容を１にと順次変更すれば，セキュリティ領域情報は，２，３と変化する。

【００６０】〔第４の実施の形態〕第４の実施の形態は，記憶媒体３０の書き換え可能領域３３中にコンテンツ利用可能状態管理テーブルを持つ場合で，書き換え可能領域３３中のコンテンツを暗号鍵で暗号化している場合の例である。

【００６１】記憶媒体３０の書き換え可能領域３３には，あらかじめ暗号化された暗号化コンテンツと，その復号鍵を記憶媒体３０の媒体固有情報で暗号化した変形復号鍵と，この変形コンテンツの利用可能状態を管理するコンテンツ利用可能状態管理テーブルが保存されているものとする。今回再生対象とするコンテンツの残り利

用回数は３であるものとする。また，記憶媒体３０のセキュリティ領域３２の情報は０であるものとする。

【００６２】このコンテンツを再生するときの例について説明する。まず，セキュリティ領域情報読み出し・書き込み部１１２を利用して記憶媒体３０のセキュリティ領域３２の情報を読み出す（この時点の情報は０）。また，管理テーブル読み出し・書き込み部１１７を利用してコンテンツ利用可能状態管理テーブルを読み出す（この時点で再生対象コンテンツの再生残り利用回数は３）。そして，読み出したセキュリティ領域３２の情報とコンテンツ利用可能状態管理テーブルと変形コンテンツを利用して，コンテンツ利用可能状態確認部１１３において，再生するコンテンツが利用可能状態にあるかどうかを確認する。

【００６３】コンテンツが利用可能状態であった場合，媒体固有情報読み出し部１１４で記憶媒体３０の媒体固有情報３１を読み出し，この媒体固有情報３１と変形復号鍵と暗号化コンテンツを利用し，コンテンツ再生部１１６でコンテンツを再生する。また管理テーブルバインド・復元部１１５でセキュリティ領域情報を利用して，コンテンツ利用可能状態管理テーブルのバインドを復元する。そして管理テーブル読み出し・書き込み部１１７を利用して，コンテンツ利用可能状態管理テーブル内の再生したコンテンツの残り利用回数を書き換える（残り利用回数＝２）。書き換えのタイミングは，再生を始めたとき，あるいは再生が最後まで終わったとき，あるいは情報提供者の指定したタイミングであるものとする。

【００６４】さらに記憶媒体３０のセキュリティ領域３２の情報を書き換え（この時点の情報は１），管理テーブルバインド・復元部１１５でこの書き換え後の情報を利用して記憶媒体３０上コンテンツ利用可能状態管理テーブルを再バインドする。

【００６５】

【発明の効果】以上説明したように，本発明によれば，記憶媒体上でコンテンツを利用する前にそのコンテンツのバックアップが他の記憶媒体に取られていたとしても，利用の際にセキュリティ領域の情報が変化し，利用可能状態がその情報に基づいてバインドし直されるため，そのバックアップコンテンツを記憶媒体に戻したときに利用不可能になり，リプレイアタックを防せぐことができるようになる。

【図面の簡単な説明】

【図１】本発明の構成例を示す図である。

【図２】第１および第２の実施の形態に係るコンテンツ再生装置の構成例を示す図である。

【図３】コンテンツ再生装置の処理フローチャートである。

【図４】バインドの例を示す図である。

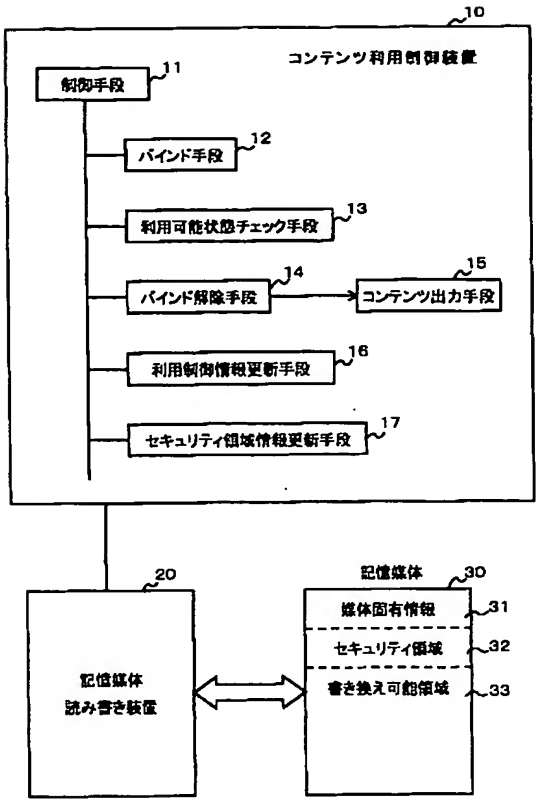
【図５】第３および第４の実施の形態に係るコンテンツ再生装置の構成例を示す図である。

【図６】コンテンツ利用可能状態管理テーブルの構成例を示す図である。

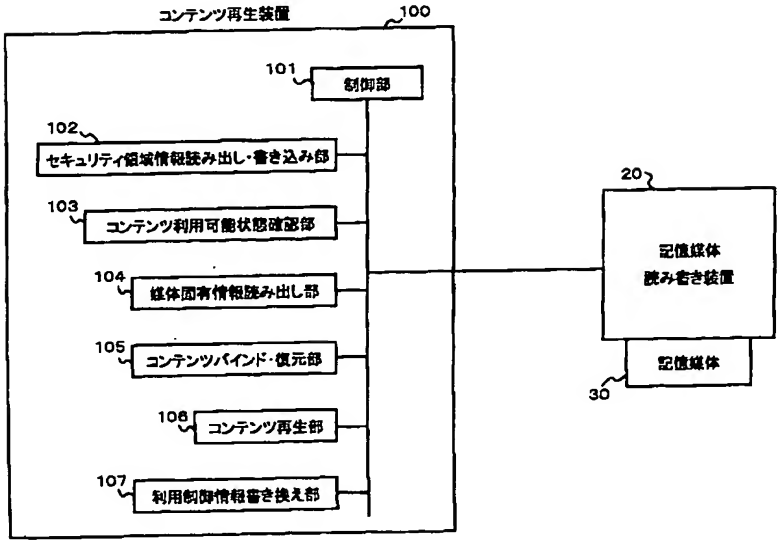
【符号の説明】

１０　コンテンツ利用制御装置
１１　制御手段
１２　バインド手段
１３　利用可能状態チェック手段
１４　バインド解除手段
１５　コンテンツ出力手段
１６　利用制御情報更新手段
１７　セキュリティ領域情報更新手段
２０　記憶媒体読み書き装置
３０　記憶媒体
３１　媒体固有情報
３２　セキュリティ領域
３３　書き換え可能領域

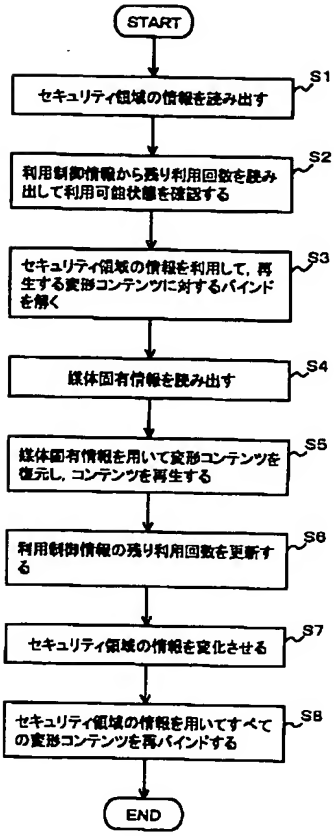
【図１】


10
コンテンツ利用制御装置
制御手段
11
バインド手段
12
利用可能状態チェック手段
13
バインド解除手段
14
コンテンツ出力手段
15
利用制御情報更新手段
16
セキュリティ領域情報更新手段
17
20
記憶媒体
読み書き装置
記憶媒体
30
媒体固有情報
31
セキュリティ領域
32
書き換え可能領域
33

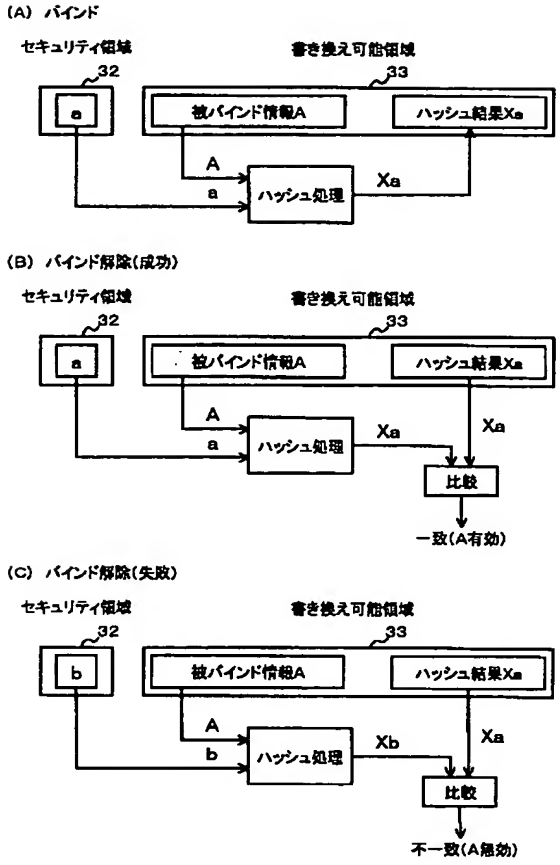
【図２】


コンテンツ再生装置
100
101
制御部
102
セキュリティ領域情報読み出し・書き込み部
103
コンテンツ利用可能状態確認部
104
媒体固有情報読み出し部
105
コンテンツバインド・復元部
106
コンテンツ再生部
107
利用制御情報書き換え部
20
記憶媒体
読み書き装置
記憶媒体
30

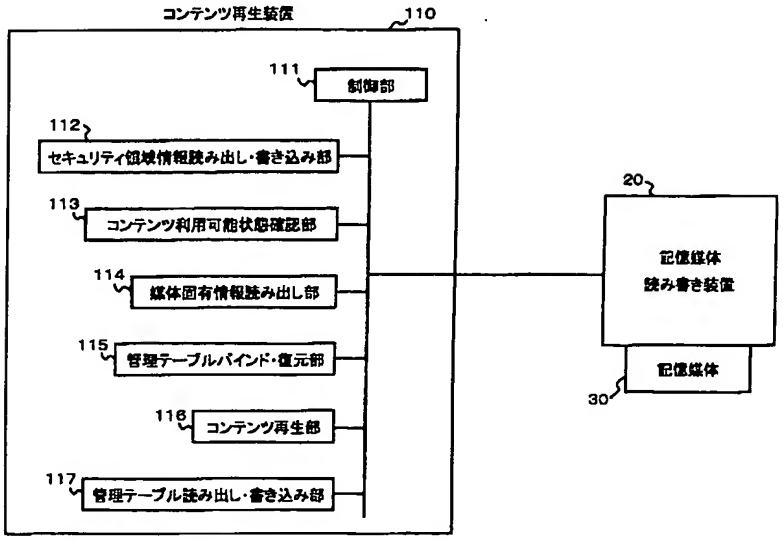
【図３】


START
セキュリティ領域の情報を読み出す
S1
利用制御情報から残り利用回数を読み出して利用可能状態を確認する
S2
セキュリティ領域の情報を利用して，再生する変形コンテンツに対するバインドを解く
S3
媒体固有情報を読み出す
S4
媒体固有情報を用いて変形コンテンツを復元し，コンテンツを再生する
S5
利用制御情報の残り利用回数を更新する
S6
セキュリティ領域の情報を変化させる
S7
セキュリティ領域の情報を用いてすべての変形コンテンツを再バインドする
S8
END

【図４】



【図５】



【図６】

コンテンツ利用可能状態管理テーブル

(A) コンテンツの利用回数ごとに情報をもつ場合

コンテンツとのリンク情報	利用可能フラグ	使用済みフラグ
コンテンツ1－1	0	1
コンテンツ1－2	1	1
コンテンツ2－1	1	1
コンテンツ2－2	1	1
コンテンツ3－1	1	1
	0	0

(B) コンテンツごとに情報をもつ場合

コンテンツとのリンク情報	利用可能回数	使用済みフラグ
コンテンツ1	1	1
コンテンツ2	2	1
コンテンツ3	1	1
	0	0
	0	0
	0	0

フロントページの続き

(72)発明者 中里 加奈
東京都千代田区大手町二丁目３番１号 日本電信電話株式会社内
(72)発明者 藤井 治彦
東京都千代田区大手町二丁目３番１号 日本電信電話株式会社内

Ｆターム(参考) 5B017 AA03 BB06 BB10 CA16
5C053 FA13 FA30 GB01 GB06 GB40 HA40 JA30
5C064 CA14 CC02 CC04
5D044 AB05 AB07 BC01 CC04 DE49 DE57 GK11 GK17